Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1249 12/03/10

~ FTC: Do Not Track Tool? ~ People Are Talking! ~ Xbox-Modding Trial!
~ Will Do Not Track Work? ~ Galaxy Tablet A Rival? ~ Spam Mastermind Trial
~ Facebook Profile Scam! ~ More Net Neutrality! ~ IE6 Usage Plummets!

~ Bait and Switch Busted! ~ Playboy Collectors HD! ~ Modding Case Botched?

-* WikiLeaks Claims DoS Victim! *-
-* WikiLeaks Downed Again by Domain! *-
-* 82 Sites Shut Down for Copyright Violation *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Well, I finally ran out of my Thanksgiving leftovers, and having a little bit of withdrawal issues! But, I'll get over it soon enough, I suppose. I hope that all of you had an enjoyable holiday, complete with fine food, family and friends.

And now it's time to focus on the current and upcoming holidays - Happy Hanukkah to those of our readers who celebrate. We've already been doing some holiday shopping, trying to get it done as quickly and painlessly as possible. We both despise going to malls and such; my wife has been doing a lot of shopping online, as she's done in the past. Like most, money is still tight around here, so we've been trying to plan accordingly. A time to pick up a few things that we need, a few that we'd like, and maybe an item or two that's "fun". And that will be it. Oh yeah, and of course we'll pick up a few gifts for the dogs; they like opening presents too!

The weather here in New England has been getting colder, but still dry for the most part. No snow yet, which is always a good thing as far as I'm concerned! Of course, I've already had the obligatory cold, and am trying to shake off the effects of another one at the moment.

Until next time...

=~=~=~=

->In This Week's Gaming Section - Judge Bars Fair Use Defense in Xbox Modding Trial!
""""""""""""""""""""""""""""""""
Xbox-Modding Judge Berates Prosecution!
Government Botches Case Against Xbox 360 Hacker!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Judge Bars Fair Use Defense in Xbox Modding Trial

A California man charged with violating the DMCA by modifying Xbox 360 consoles won t be allowed to claim "fair use" at his scheduled jury trial next week, a federal judge ruled Tuesday - a decision potentially devastating to the defense, and not particularly favorable to anyone who thinks they have the right to tinker with hardware that they ve bought and paid for.

Matthew Crippen, 28, faces three years in prison on two allegations of violating the anti-circumvention provisions of the Digital Millennium Copyright Act for financial gain. Crippen, who s from Anaheim, allegedly had a business modding Xbox 360s for between $60 and $80 a pop, allowing the consoles to run pirated games or unapproved homebrew software. He was indicted after allegedly performing the service for an undercover corporate security investigator with the Entertainment Software Association, then again for an undercover federal agent.

His trial is set to begin on November 30 in Los Angeles, and would be the first federal criminal prosecution for console-modding to reach a jury.

Crippen s lawyer hoped to convince that jury that Crippen s alleged modifications weren t intended to enable piracy, but to allow Xbox owners to make lawful "fair use" of copyrighted material, or for other non-infringing purposes. The lawyer compared modding the console to jail breaking an iPhone, an activity explicitly permitted under a recent DMCA exception approved by the U.S. Copyright Office.

"The Copyright Office cited the fact that the only way for consumers to exercise their fair-use rights by running non-Apple endorsed applications was through circumvention of access controls," wrote Callie Glanton Steele, a Los Angeles federal deputy public defender, in a court filing.

But U.S. District Judge Philip shot down that argument Tuesday, noting that the DMCA makes it a crime to "circumvent a technological measure that effectively controls access" to copyrighted material, even if there s no proof that the circumvention was intended to facilitate piracy. The iPhone exemption is irrelevant, he wrote, because the Copyright Office did not extend that exemption to game consoles - just phones.

"[A]lthough the government will have to establish that the technological measure that Mr. Crippen allegedly circumvented was used to control access to copyrighted work, the Government need not show that the modified Xbox s were actually used for infringing purposes," (.pdf) wrote Gutierrez.

The decision isn t a surprise, but it highlights the troubling conflict created by the 1998 DMCA. Copyright law still allows for the fair use of protected material - for example, an educator might be allowed to copy a brief scene from a DVD movie for classroom instruction. But if a hardware-maker deploys technology that prevents that fair use, bypassing that technology for any reason is unlawful.

Other pre-trial issues remain to be decided in the case, including the admissibility of a covert video recording of Crippen allegedly performing the modification, and whether or not the jury can hear the testimony of hardware hacking guru Andrew "Bunnie" Huang, who s agreed to testify for

the defense.

Huang told Threat Level last month that he s prepared to offer expert testimony that the Xbox 360 hack doesn t circumvent a copy control mechanism within the meaning of the DMCA. The government has asked Gutierrez to block his testimony.

Xbox-Modding Judge Berates Prosecution, Puts Trial on Hold

Opening statements in the first-of-its kind Xbox 360 criminal hacking trial were delayed here Wednesday after a federal judge unleashed a 30-minute tirade at prosecutors in open court, saying he had "serious concerns about the government s case."

"I really don t understand what we re doing here," U.S. District Judge Philip Gutierrez roared from the bench.

Gutierrez slammed the prosecution over everything from alleged unlawful behavior by government witnesses, to proposed jury instructions harmful to the defense. When the verbal assault finally subsided, federal prosecutors asked for a recess to determine whether they would offer the defendant a deal, dismiss or move forward with the case that was slated to become the first jury trial of its type. A jury was seated Tuesday.

Among the judge s host of complaints against the government was his alarm that prosecutors would put on two witnesses who may have broken the law.

One is Entertainment Software Association investigator Tony Rosario, who secretly video-recorded defendant Matthew Crippen allegedly performing the Xbox mod in Crippen s Los Angeles suburban house. The defense argues that making the recording violates California privacy law. The other witness is Microsoft security employee Ken McGrail, who analyzed the two consoles Crippen allegedly altered. McGrail admitted that he himself had modded Xboxes in college.

"Maybe two of the four government witnesses committed crimes," the judge said from the bench. "I think it is relevant and the jury is going to hear about it" - both crimes."

The government had fought to keep the witness conduct a secret from the jury.

Crippen is charged with two counts of violating the anti-circumvention provisions of the Digital Millennium Copyright Act, and faces a maximum five years for each count if convicted. The government maintains Crippen, a hotel car-parking manager, ran a small business from his Anaheim home modifying the firmware on Xbox 360 optical drives to make them capable of running pirated copies of games.

The judge on Wednesday even backtracked on an earlier ruling that had prohibited Crippen, 28, from raising a "fair use" defense at trial.

Crippen was hoping to argue to jurors that it was legal to hack the consoles because the modification had non-infringing purposes, like allowing the machines to run homebrew software, or permitting limited fair use of copyright material such as backup copies of video games.

While the judge ruled last week that such a defense was not permitted by the DMCA, he seemingly changed course during his speech.

"The only way to be able to play copied games is to circumvent the technology," Gutierrez said. "How about backup games and the homebrewed?"

The fair-use issue came up as the judge berated prosecutor Allen Chiu s proposed jury instructions, which included the assertion that the government need not prove that Crippen "willfully" breached the law, in what is known as "mens rea" in legal parlance. The judge noted that the government s own intellectual property crimes manual concerning the 1998 DMCA says the defendant has to have some knowledge that he was breaking the law.

"The first prosecution 12 years later, and you re suggesting a mens rea that is akin to exactly contrary to the IP manual: that ignorance of the law is no excuse?" the judge barked.

"You didn t even propose a middle ground," Gutierrez continued. "What s getting me more riled, it seems to me I cannot communicate the severity to you of what s going on here."

As the judge worked through his laundry list of complaints over the prosecution, word of the unusual judicial rebuke spread through the courthouse, drawing a trickle of about a dozen prosecutors and defense attorneys into the courtroom to watch from the gallery.

"I apologize to the court," Chiu said at the end.

Court is recessed until 1:30 p.m.

Government Botches Case Against Xbox 360 Hacker, Drops Charges

A 28-year-old Southern California man facing up to 10 years in prison for allegedly modifying Xbox 360s to play illegal versions of games is free and clear after federal authorities abruptly dropped their case against him.

Opening statements in the trial were delayed yesterday after the judge hearing the case verbally flayed the prosecution, admitting he had "serious concerns about the government’s case," and at one point stating "I really don’t understand what we’re doing here."

The case against Matthew Crippen, a hotel valet service manager alleged to have run a side business modifying Xbox 360s to play pirated games, was the first of its kind to come to trial.

Make that the first of its kind to also get pushed off a cliff. According to Wired, the government bailed yesterday, telling the judge its decision to withdraw was "based on fairness and justice."

Things fell apart on Wednesday as the government opted to proceed with opening testimony. Tony Rosario, its first witness and an undercover agent with the Entertainment Software Association, added a testimonial wrinkle it failed to disclose to the defense--that Crippen had placed a copy of a pirated video game into an Xbox 360 to verify his modification was working.

The prosecution then moved to dismiss the case, admitting its error, though the reversal wasn't a tacit admission of defeat. The case was dropped on a technicality, not on its merits in relation to the Digital Millennium Copyright Act, which among other things attempts to criminalize the modification of technology to circumvent copyright protection measures. This case, had it gone forward, would have been the first to test the DMCA's application to modified game consoles.

In other words, not the first or last we've heard of it.

While it's routinely assumed modifications to game consoles exist to circumvent piracy measures, some have lobbied against the DMCA because of its potential to stifle creativity. For instance, modified game consoles can also be used to engage legitimate software crafted by a community of enthusiasts. Removing that ability, some say, would be like outlawing aftermarket modifications to just about anything.

What's the difference between modifying an Xbox 360 to enable supplemental functionality and jail-breaking an iPhone, something already considered legal "fair use" in the United States?

Downloading and playing pirated games is illegal, there's no ambiguity on that point. But modifying technology to unlock additional functionality falls in a different column, whether you're arguing on legal or philosophical grounds.

No one likes to be told what they can and can't do with something they've purchased. Applying the DMCA to console modification would open the door for protectionists (private or governmental) to start locking down the games industry. That's the wrong approach, as far as I'm concerned, especially as piracy-proof distribution mediums increase in popularity, from "games-on-demand" digital downloads through Steam or Xbox Live Marketplace, to playing "in the cloud" with distributed computing services like OnLive.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

WikiLeaks Says Was Denial-of-Service Attack Victim

The online website WikiLeaks on Sunday blamed the temporary outage of its site on a denial-of-service attack by unknown hackers trying to prevent its release of hundreds of thousands of classified U.S. State Department documents.

WikiLeaks said on Twitter early Sunday that its website was "under a mass distributed denial of service attack" but promised that Spain's El Pais, France's Le Monde, Germany's Der Spiegel, Britain's Guardian newspaper and The New York Times "will publish many US embassy cables tonight, even if

WikiLeaks goes down." WikiLeaks had given the media outlets prior access to the diplomatic cables to publish in conjunction with their Sunday release on its site.

There was no reason to doubt WikiLeaks' claim; the website was inaccessible for much of Sunday, though several hundred cables were posted on its site by late afternoon. The cables, many of them classified, offer candid, sometimes unflattering assessments of foreign leaders, ranging from U.S. allies such as Germany and Italy to other nations like Libya, Iran and Afghanistan.

In a typical denial-of-service attack, remote computers commandeered by rogue programs bombard a website with so many data packets that it becomes overwhelmed and unavailable to visitors. Pinpointing the culprits is impossible because the Internet's structure does not allow for the tracing back of the data packets used in such attacks, computer security expert Bruce Schneier told The Associated Press on Sunday.

Hackers have used denial-of-service attacks over the years to target corporate and government websites.

Last month political bloggers in Vietnam said they were victimized by cyberattacks designed to block their websites to stifle government dissent. Other targets have included U.S. and South Korean government websites in 2009 and computer networks in Estonia, which were crippled for nearly three weeks in 2007 by what were believed to be Russian hackers.

In the weeks leading up to the 2008 war between Russia and Georgia, Georgian government and corporate websites were hit with denial-of-service attacks. The Kremlin denied involvement.

James Lewis, a cybersecurity expert and a senior fellow at the Center for Strategic and International Studies, said it's unlikely the U.S. or some other government would use denial-of-service attacks against WikiLeaks.

His best guess is it's "a bunch of geeks who've decided they're annoyed with WikiLeaks."

"Denial of service is usually the amateur's approach," he told the AP on Sunday. "Usually it's the hacker community ..."

Lewis said he's never heard of the U.S. trying to attack a website like this.

"Usually they're more interested in exploiting, that is getting into WikiLeaks to figure out what's going on. Or they're interested in doing some kind of damage, and denial of service really doesn't do any damage."

Such an attack would only stall WikiLeaks, not prevent the information from being released.

Schneier also said he seriously doubts any U.S. government agency would be involved in such an attack because it amounts to a mere "nuisance" and could not stop Wikileaks from releasing the diplomatic cables. He notes that there are many ways to distribute information online.

An encrypted file that was made available online using BitTorrent file-sharing technology in late July is believed to hold the cables. All Wikileaks would need to do to unlock the file is distribute the key.

WikiLeaks.org Downed by Domain Hosting Service

WikiLeaks' main website could not be accessed on Friday through its WikiLeaks.org domain name after a subsidiary of Dynamic Network Services terminated its domain name service.

Dynamic Network Services' subsidiary, EveryDNS.net, terminated the WikiLeaks.org domain name because repeated DDOS (Distributed Denial of Service) attacks against WikiLeaks "have, and future attacks would, threaten the stability of the EveryDNS.net infrastructure, which enables access to almost 500,000 other websites," it said on its website.

EveryDNS.net said it notified WikiLeaks by email, Twitter and the chat function available through the WikiLeaks.org website that its domain name service would be terminated in 24-hours. That 24-hour period ended Dec. 2 at 10 p.m. Eastern Standard Time in the U.S.

"Any downtime of the Wikileaks.org website has resulted from its failure to use another hosted DNS service provider," EveryDNS.net said.

WikiLeaks put out a note on Twitter saying, "WikiLeaks,org domain killed by U.S. EveryDNS.net after claimed mass attacks," and implored supporters to keep WikiLeaks strong with continued donations.

The WikiLeaks comment appeared at odds with an earlier WikiLeaks Twitter post saying that DDOS attacks against its servers reached 10 Gigabits per second on Nov. 30. Amazon Web Services also confirmed the DDOS attacks, saying in a blog posting that, "There were indeed large-scale DDOS attacks, but they were successfully defended against."

The domain name service termination comes just days after Amazon Web Services stopped hosting WikiLeaks on its servers for breaking user rules saying that websites must use their own content and not carry data that might injure others. The U.S. Homeland Security and Governmental Affairs Committee, chaired by Senator Joe Lieberman, had also asked Amazon to stop hosting the controversial
website.

WikiLeaks has come under fire for publishing classified U.S. documents, including videos and documents from the wars in Iraq and Afghanistan as well as sensitive cables sent between U.S. embassies and the U.S. State Department. WikiLeaks continues to post the cables.

Dynamic Network Services is a U.S. company based in Manchester, New Hampshire. Its EveryDNS.net subsidiary said all of its systems were functioning normally.

FTC Proposes Do Not Track Tool for Web Marketing

Federal regulators are proposing to create a "Do Not Track" tool for the Internet so that consumers could prevent marketers from tracking their Web browsing habits and other behavior in order to target advertising.

The proposal, inspired by the government's existing "Do Not Call" registry

for telemarketers, is among the recommendations outlined in a privacy report released Wednesday by the Federal Trade Commission. The report lays out a broad framework for protecting consumer privacy both online and offline as personal data collection becomes ubiquitous - often without consumer knowledge.

The FTC hopes the report will help guide the marketing industry as it develops self-regulatory principles to define acceptable corporate behavior. The FTC also is trying to influence lawmakers and other policymakers as they draft new rules of the road to protect privacy. The agency has limited authority to write those rules itself, so new regulations would likely require congressional action.

Protecting consumer privacy, the agency says, is critical since marketers - particularly online marketers - are increasingly analyzing the websites that consumers visit, the links they click, Internet searches, online and offline purchases, the physical locations of wireless devices and all sorts of personal information disclosed on social networking sites.

So far, FTC chairman Jon Leibowitz said Wednesday, the marketing industry has not done nearly enough to ensure that consumers understand what personal information is being collected about them or to give them adequate control over that data collection.

The agency envisions a Do Not Track tool as one important way to let consumers decline, or "opt out" of, much of the tracking that occurs online - a practice the industry calls behavioral advertising. The tool would most likely take the form of a browser setting that would apply across the board as consumers jump from site to site. It would clearly inform sites when tracking and targeted advertising are off limits for a particular browser.

The concept is loosely based on the FTC’s National Do Not Call Registry, which was launched in 2003 and has been widely credited for allowing Americans to eat their suppers in peace. More than 190 million people have listed their phones on the registry, which prohibits calls from telemarketers. Violating the registry subjects telemarketers to civil penalties up to $16,000 per violation.

Leibowitz, who first floated the idea of Do Not Track last summer, said that although the technology has not yet been widely deployed for consumers, browser companies are experimenting with it. And lawmakers do appear interested in the concept. Bobby Rush, chairman of the House Commerce subcommittee that deals with consumer protection issues, will hold a hearing on potential Do Not Track legislation on Thursday.

The new FTC report comes at time of mounting concern about Internet privacy in both Washington and Europe.

The National Information and Telecommunications Administration, part of the Commerce Department, is also preparing a report on the issue. And the Obama administration’s Office of Science Technology Policy has created a new group to develop broad principles on online privacy to guide legislative action and regulatory policy.

Meanwhile, last month the European Union said it plans to update its privacy regulations to give consumers more control over online tracking.

Will A ’Do Not Track’ Browser Option Protect Your Privacy?

The Federal Trade Commission on Thursday provided more details on its "do not track" browser proposal, though it was met with skepticism by security experts at Symantec.

David Vladeck, director of the FTC’s Bureau of Consumer Protection, told the House Energy and Commerce Committee that a "do not track" option would be a "more uniform and comprehensive consumer choice mechanism for online behavioral advertising" than the options currently available.

Joe Pasqua, vice president of research at Symantec, however, said the idea is "conceptually reasonable but technically difficult."

Vladeck appeared on Capitol Hill one day after the FTC unveiled a broad plan for online privacy, which included the "do not track" provision. Basically, it suggests that browser companies add a feature that allows users to surf the Web without having any of their activities tracked; no information sent to advertisers or data miners, for example.

At this point, the FTC plan is just a proposal and not enforceable. The agency is asking for stakeholders to submit comments on the plan by January, and it will issue a revised proposal sometime next year. The FTC said its ideas could be used as best practices as Congress considers online privacy legislation, however, which is why Vladeck appeared before the committee on Thursday.

"The most practical method of providing uniform choice for online behavioral advertising would likely involve placing a setting similar to a persistent cookie on a consumer’s browser, and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements," Vladeck said. "To be effective, there must be an enforceable requirement that sites honor those choices."

Most browsers offer private browsing features, which do not track user activity, but Vladeck pushed for mechanisms that are "more clear, easy-to-locate, and effective."

If Congress does choose to take up the issue, Vladeck asked members to consider several issues: bills should not undermine online behavioral advertising entirely since some consumers do benefit from it; it would not operate like the "do not call" program since there is no persistent identifier for computers like phone numbers (IP addresses change); and the FTC should have the authority to enforce the legislation and impose civil penalties.

Also in attendance was Daniel Weitzner from the National Telecommunications and Information Administration (NTIA) within the Commerce Department. He acknowledged that users currently have the option to avoid tracking through private browsing features, and issued support for a "voluntary, multi-stakeholder process, backed up, in the end, by FTC enforcement of the privacy commitments made to consumers through such a system."

The Commerce Department’s Internet Policy Task Force, meanwhile, will also "start to convene industry and consumer groups to discuss the next steps toward achieving voluntary agreements on implementation methods for a do-not-track requirement," Weitzner said.

Symantec’s Pasqua, however, was doubtful. "We are unsure exactly how a Do-Not-Track mechanism would be all that different from the opt-out link currently offered by the Network Advertising Initiative (NAI)," he said. "Perhaps the most significant difference might be that the NAI includes only a limited number of companies, but a Do-Not-Track registry would presumably be universal."

"Our vision is for a future where individuals can voluntarily choose to obtain a secure, interoperable, and privacy-enhancing credential such as a smart identity card or a digital certificate on a cell phone, from a variety of public and private service providers, to authenticate themselves online for different types of transactions," Pasqua said.

Deciding what is intrusive is also an issue, he continued. "What one user considers excessive tracking might be completely reasonable to others."

Browser companies like Google, Microsoft, and Mozilla have all pledged to review the FTC’s privacy plan and consider its suggestions.

FCC Net Neutrality Plan Faces Battle with GOP

Just hours after the head of the Federal Communications Commission said he would push ahead with rules to prohibit broadband providers from blocking or discriminating against Internet traffic flowing over their networks, the battle lines are being drawn.

The proposal has won grudging support from several big phone and cable companies, including AT&T Inc. and Comcast Corp., and at least a few public interest groups. It faces withering criticism from Republicans in Congress and at the FCC, who are calling it an effort to regulate the Internet.

But the fate of the "network neutrality" plan crafted by FCC Chairman Julius Genachowski may ultimately lie with his two fellow Democrats on the five-member commission. For now, it’s unclear how they will vote when the agency considers the proposal later this month.

"Today is the beginning of an important discussion, and not the end," one of those two commissioners, Michael Copps, said in a statement Wednesday. "At issue is who will control access to the online experiences of consumers - consumers themselves or Big Phone and Big Cable gatekeepers."

Genachowski’s widely anticipated plan, which he laid out in a speech Wednesday, is the product of months of negotiations to find middle ground in a policy dispute that pitted phone and cable giants against a number of Internet companies and public interest groups. Net neutrality rules were one of the Obama administration’s top campaign pledges to the technology industry and have been among Genachowski’s priorities since he took over the FCC more than a year ago.

Many big Internet companies, such as search leader Google Inc. and calling service Skype, insist regulations are needed to ensure broadband companies can’t use their control over Internet connections to dictate where consumers can go and what they can do online. They are particularly concerned that without strong net neutrality protections, phone and cable companies could slow or block online phone calls, Web video and other

Internet services that compete with their core businesses. Internet companies and public interest groups also want regulations to prevent broadband providers from favoring their own online traffic or traffic from business partners that can pay to take priority over other online services.

But Genachowski has fought an uphill battle against phone and cable giants, which insist they need flexibility to manage network traffic so that high-bandwidth applications - such as online video - don't hog capacity and slow down their networks. The communications companies also argue that after spending billions to upgrade their lines for broadband, they need to be able earn a healthy return by offering premium high-speed services. They warn that burdensome regulations would discourage them from continuing to invest in their systems.

Genachowski's plan, which builds on a set of FCC principles established under the previous administration in 2005, would require that broadband providers let subscribers access all legal online content, applications and services over their wireline networks. But it contains several key concessions to the phone and cable companies.

For one thing, it would give broadband providers flexibility to manage their systems to deal with problems such as network congestion and unwanted traffic including spam as long as they publicly disclose their network management practices.

The proposal would give wireless carriers even more leeway to manage data traffic, since wireless systems have more bandwidth constraints than wired networks. It would, however, prohibit wireless carriers from blocking access to any websites or competing applications such as Internet calling services on mobile devices, and would also require the carriers to disclose their network management practices.

In addition, the proposal would let broadband providers experiment with routing traffic from specialized services such as smart energy grids and home security systems over dedicated networks, as long as the practice doesn't slow down the public Internet.

The proposal drew cautious praise from AT&T, which said, "The FCC appears to be embracing a compromise solution that is sensitive to the dynamics of investment in a difficult economy and appears to avoid over-regulation."

Comcast, too, said the plan "strikes a workable balance between the needs of the marketplace and the certainty that carefully-crafted and limited rules can provide to ensure that Internet freedom and openness are preserved."

Reaction among public interest groups was more mixed. Although several said they could support the proposal, one key group, Free Press, denounced it as "fake" net neutrality that would provide less protection for wireless consumers at a time when more Americans are going online using mobile devices. Free Press also said allowing dedicated networks for certain services could lead to a two-tiered Internet with a fast lane for companies that can pay for priority and a slow lane for everyone else.

In one other key concession to the phone and cable companies, Genachowski's proposal would leave in place the FCC's current regulatory framework for broadband, which treats broadband as a lightly regulated "information service."

The agency has been trying to come up with a new framework since a federal appeals court in April ruled that the FCC had overstepped its existing authority in sanctioning Comcast for discriminating against Internet file-sharing traffic on its network. Comcast's behavior violated the very net neutrality principles that Genachowski now hopes to adopt as formal rules.

To ensure that the commission would be on solid legal ground in adopting net neutrality rules and other broadband regulations following that decision, Genachowski had proposed redefining broadband as a telecommunications service subject to "common carrier" obligations to treat all traffic equally. But that effort triggered a fierce backlash from the phone and cable companies, as well as from many Republicans in Congress, prompting Genachowski to back down.

His new plan is based in large part on a proposal that Rep. Henry Waxman, D-Calif., the outgoing chairman of the House Commerce Committee, unsuccessfully tried to push in Congress several months ago. Waxman, too, ran into opposition from Republicans who say net neutrality rules amount to unnecessary regulation.

Republicans went on the attack again Wednesday against Genachowski's latest proposal. Robert McDowell and Meredith Attwell Baker, the two Republicans on the FCC, said they could not support the proposal. McDowell said Genachowski's effort "to adopt sweeping regulations of Internet network management" is an "ill-advised maneuver."

And two top Republicans on the House Commerce Committee, Joe Barton of Texas and Cliff Stearns of Florida, sent a letter to the FCC chairman asking him to explain where the agency gets authority to mandate net neutrality.

With Republicans set to take over the House next year, Genachowski is certain to face even more resistance in the next Congress, adding to pressure on the chairman to get his plan through the FCC this month.

Courts Shut Down 82 Sites for Alleged Copyright Violations

Two U.S. government agencies have obtained seizure orders from courts across the nation for the domain names of 82 websites accused of selling products that infringe copyright law, including music, movies and handbags.

The seizure orders, from courts in eight states and Washington, D.C., have allowed the U.S. Department of Justice and the U.S. Department of Homeland Security's Immigration and Customs Enforcement (ICE) to shut down sites including Torrent-finder.com, DVDscollection.com, Sunglasses-mall.com, and NFLjerseysupply.com, officials from the agencies said Monday.

News reports of multiple site closures surfaced in the last few days, but officials with the two agencies talked about the actions during a press conference Monday.

"With today's seizures, we are disrupting the sale of thousands of counterfeit items," U.S. Attorney General Eric Holder said. "We are cutting off funds to those looking to profit from the sale of illegal

goods and exploit the ingenuity of others. And, as the holiday shopping season gets underway, we are also reminding consumers to exercise caution when looking for deals and discounts online. To put it simply: If a deal seems too good to be true, it probably is."

Sites targeted by the two agencies displayed a notice on their home pages saying that ICE had seized the domain names. "Willful copyright infringement is a federal crime that carries penalties for first time offenders of up to five years in federal prison, a $250,000 fine, forfeiture and restitution," the notices read. "Intentionally and knowingly trafficking in counterfeit goods is a federal crime that carries penalties for first time offenders of up to ten years in federal prison, a $2,000,000 fine, forfeiture and restitution."

Some commentators questioned the seizure of Torrent-finder.com, a search engine for BitTorrent files that didn't host any files itself. Another version of the site remained online at Torrent-finder.info Monday morning.

ICE "went way beyond its mandate to seize a whole bunch of domain names," wrote Mike Masnick, founder of the TechDirt blog. "Many of the operators of the domain names seized in this round state they hadn't received any notification of complaints, let alone demands to be taken down."

The seizure of search engines is "ridiculous," Masnick added. "For anyone who actually understands how the internet works (i.e., clearly not Homeland Security) this is a massively troubling move, suggesting that if Homeland Security doesn't like how your search engine works, it can simply seize your domain and put up a really scary looking graphic, claiming it has taken over your website," he wrote.

Senator Patrick Leahy, a Vermont Democrat and chairman of the Senate Judiciary Committee, praised the action by the DOJ and ICE. The seizures targeted "rogue websites," said Leahy, who has sponsored legislation this year that would make it easier for the DOJ to shut down infringing websites.

"The innovative use of the tools currently available to law enforcement to seize these domain names is similar to the remedy that would be specifically authorized under the bipartisan Combating Online Infringement and Counterfeits Act for websites that are registered in the United States," Leahy said in a statement. "We can no longer sit on the sidelines while American intellectual property is stolen and sold online using our own infrastructure. This costs American jobs, hurts our economy, and puts consumers at risk."

Also cheering the seizures was Mitch Bainwol chairman and CEO of the Recording Industry Association of America.

"Federal law enforcement authorities have now hung a 'closed for business' sign on some of the most notorious music websites that were havens for copyright theft," he said in a statement. "No anti-piracy initiative is a silver bullet, but targeted government enforcement against the worst of the worst rogue sites sends a strong message that illegally trafficking in creative works carries real consequences and won't be tolerated."

Man Pleads Not Guilty to Running Vast Spam Network

A 23-year-old Russian man accused of masterminding a vast worldwide spamming network pleaded not guilty Friday in federal court in Wisconsin to violating a U.S. anti-spam law.

The judge ordered Oleg Y. Nikolaenko held without bond, saying he was a flight risk because of his access to cash and his lack of ties to Wisconsin or the U.S.

Nikolaenko was brought into court wearing bright orange prison pants and matching sweatshirt and shackled at the ankles. His attorney entered the plea as a Russian interpreter translated for the Moscow man.

Prosecutors say Nikolaenko ran a network that involved placing malicious code on unsuspecting users' computers and then hijacking the infected machines to blast out billions of e-mails.

Internet security experts say the network was so massive that on some days it accounted for one of every three unwanted e-mails in the world.

Nikolaenko is charged with violating the CAN-SPAM act by intentionally falsifying header information in commercial e-mail messages and sending at least 2,500 spam e-mails per day, the minimum threshold for the charge. Prosecutors say his network was capable of sending up to 10 billion messages per day.

The charge carries a maximum penalty of three years in prison and a $250,000 fine.

Nikolaenko, unshaven with disheveled hair, sat silent and expressionless during the 20-minute proceedings.

His attorney, Christopher Van Wagner, said he intended to mount a vigorous defense and would examine whether broad pre-trial publicity might jeopardize his client's ability to receive a fair trial.

"Some people still harbor Cold War images of people from Russia," he told reporters on the courthouse steps. "You take one look at Oleg, he looks like a kid you find in a basement munching nachos and playing Wii" video games.

Assistant U.S. Attorney Erica O'Neil said the prosecution's case would hinge on "voluminous" records including e-mails Nikolaenko allegedly sent and information gleaned from computer hard drives. She said a computer-crimes expert from the U.S. Department of Justice is assisting because of the complexity of the case.

Van Wagner hinted that he may try to cast doubt on the validity of the e-mail records.

"When you respond to an e-mail you don't know who's typing it," he said.

Nikolaenko was arrested last month at the Bellagio Hotel while he was in Las Vegas for a car show. He is being tried in Milwaukee because that's where an undercover FBI investigator ordered Viagra through an e-mail distributed by Nikolaenko's alleged operation and received bogus herbal pills instead, an FBI spokesman said.

O'Neil said Nikolaenko is being held at a U.S. Marshal detention facility in Milwaukee.

In arguing that Nikolaenko should be granted release on bail, Van Wagner noted that his client's wife and young daughter were in the process of requesting travel visas in Russia so they could be with Nikolaenko in Milwaukee for the trial. They wouldn't be doing that if Nikolaenko were planning to flee, he said.

But U.S. Magistrate Judge Patricia Gorence wasn't convinced, saying Nikolaenko had two passports and $4,000 in cash when he was arrested. She said Van Wagner could request a new bond hearing once the defense arranged for a place for Nikolaenko to live, a request Van Wagner said he would "absolutely" make.

Prosecutors say they sniffed out Nikolaenko's trail during the prosecution of another man convicted in Missouri of conspiring to traffic in counterfeit Rolex watches. The say details emerged that led them on a far-flung investigation that eventually helped them tie Nikolaenko to one of the most sophisticated spamming networks in the world - "Mega-D," which investigators said accounted for 32 percent of all worldwide spam.

Investigators say Mega-D was a botnet, short for "robot network," in which users' computers are infected with so-called malware that allows someone to remotely hijack the computer and have it send out spam e-mails. The Mega-D network included more than half a million infected computers.

Nikolaenko is due in court Dec. 21 for a scheduling conference. Gorence said his trial must start no later than Feb. 11.

Facebook Scam: 'See Who Has Viewed Your Profile'

Curious to see who views your Facebook profile page?

You're out of luck. Status updates, Facebook groups, and pages claiming to let users see who has viewed their Facebook profile pages are scams, often linking users to ad-filled sites.

In recent days, for instance, you may have seen your Facebook friends speaking in bizarrely adolescent chatroom vernacular:

"OMG OMG OMG... I cant believe this actually works! Now you really can see who viewed your profile! on [LINK]."

"If you're tempted to click on the link, you're taken to a webpage that encourages you to go a little deeper and permit an application to have access to your Facebook profile," wrote Graham Cluley, a senior technology consultant at Sophos, in a blog post.

According to Sophos, over 60,000 people clicked into the claim in a few hours.

But as Facebook noted in July, there is no way anyone can see who has viewed their profile, and no way others can create such a function.

"We're working hard to block and remove websites, Pages, and applications that claim to do this. If you see one, don't be fooled, and report it to us immediately," the company wrote on its security page.

Clicking into these links usually directs people to ad-filled pages. Others might promise to exchange a profile-viewing feature if a user can generate enough likes and linkshares.

"If you've been hit by a scam like this, remove references to it from your newsfeed, and revoke the right of rogue applications to access your profile via Account/ Privacy Settings/ Applications and Websites," Cluley suggests.

Senate Passes Bill to Protect Online Shoppers from Bait and Switch Tactics

A bill to protect online shoppers from bait-and-switch scams was approved Wednesday by the U.S. Senate. The measure is aimed at a practice called "post transaction advertising" that has bilked millions of Americans of billions of dollars by secretly subscribing them to services without their consent.

"This is a victory for American consumers," declared Sen. John D. (Jay) Rockefeller (D-W. Va.) in a statement. "This bipartisan legislation provides new standards that make sure businesses can't bill online shoppers for services they did not want to buy."

The legislation was drafted after an extensive probe by the Senate Commerce, Science and Transportation committee, which Rockefeller chairs.

"Last year, the committee learned that unscrupulous businesses used offers of rebates and rewards as a smokescreen to pick the pockets of millions of online shoppers," he said. "It's not the way business should be done in America and it will end. We're slamming the door on this billion dollar scam."

The sales tactic, used by companies like Affinion, Vertue and Webloyalty, works like this. Following checkout after buying something at a website, a shopper is offered some kind of perk - free shipping or a cash rebate. When the shopper accepts the offer, they're automatically enrolled in some kind of subscription service without their knowledge and their credit is charged for it.

The tactic works because hundreds of shopping sites were willing to share their customers' billing information with the companies for a cut of the action.

Under the bill, called the Restore Online Shoppers' Confidence Act, the following protections would become law:

* Companies would be prohibited from using misleading post-transaction advertisements by requiring them to clearly disclose the terms of their offers, and to obtain billing information, including full credit or debit card numbers, directly from consumers.

* Internet retailers and other commercial websites would be prohibited from transferring a consumer's billing information, including credit and debit card numbers, to post-transaction third party sellers.

* Companies that use negative options" on the Internet would be required to meet certain minimum disclosure and enrollment requirements, so consumers will not end up paying recurring fees for goods and services they did not intend to purchase.

The bill now goes to the House for action.

iPad Has Real Xmas Rival in Galaxy Tablet

Last Christmas anybody asked if they wanted a "tablet" probably thought they were being offered a pill to ease indigestion caused by a little bit of festive over-indulgence.

But this year, millions of people around the world will be glued to their iPad or other tablet computer instead of watching yet another re-run of a movie on TV.

Samsung Electronics says it has sold over 700,000 of its Galaxy Tab device in the six weeks since its launch and believes at least a million will be in people's hands by the end of the year.

But that's still miles behind the iPad, which only went on sale in South Korea - Samsung's home turf - for the first time on Tuesday.

Apple has sold more than eight million of the gadgets since it went on sale in April but could have sold more, experts say, were it not for problems making enough to meet demand.

Sony, BlackBerry maker Research In Motion (RIM), Toshiba, Hewlett-Packard, Motorola, Dell, Asus, Acer - most of the big global brand names in the technology sector have a tablet computer on the market or in the pipeline.

Technology research firm Gartner last month said sales of tablet computers are expected to soar from nearly 20 million units this year to 55 million next year and over 208 million in 2014.

The Galaxy Tab has a seven-inch (18-centimetre) touch screen - significantly smaller than the iPad's nearly 10-inch display. But Samsung says it will introduce "new tablets of different sizes in the near future".

Apple's first generation iPad does not have a camera, does not function as a phone and the company does not allow the Flash video standard on the gadget.

These are all big advantages for Samsung, the company says.

"The Tab sets itself apart from other similar smart media devices by featuring optimal portability, Flash support, dual cameras and phone-call functions," Samsung Electronics spokesman Nam Ki-yung told AFP

"Owning a Tab is like having your personal library, entertainment system, office workstation and e-learning resources rolled into one device - that snugly fits into your pocket."

While Apple has its own App store where iPad owners can buy software and

games to run on its array of gadgets, Samsung and most other tablets run on Google’s Android, with apps available from the Android Market store.

Sales in tablet computers should see exponential growth in the next 12 months, analysts say.

"Tablets are basically new creatures," Young Park, a tech analyst for South Korea’s Woori Investment and Securities, told AFP.

"So this is a brand new market which is set to grow substantially. It will be interesting to watch how the market evolves over the next year or so.

"As more and more tablet devices come onto the market, that will inevitably eat into Apple’s lead."

Sales of tablet computers, Hong Kong-based Young believes, will remain steady during the run up to Christmas but will not increase significantly.

"A tablet computer such as Apple’s iPad or the Samsung Galaxy Tab is hard to give as a Christmas gift," Young said.

"The main problem is most of them require a subscription with a network and you have to sign a 12 or even 24 month contract. That makes it difficult to give as a surprise. Plus, they’re not cheap."

The cheapest iPad costs 499 dollars in the US while the top model is priced at 829 dollars. Samsung’s Galaxy Tab costs around 600 dollars, when bought without a subscription to a network.

Playboy Releases Back Issues on Hard Disk

Struggling to stay relevant in the Internet era. Well, Hef and Co. have come up with a revenue booster just in time for the stocking-stuffer season: 56 years of Playboy on a 250GB hard drive.

The "collector’s edition" costs $300 and includes every print issue from December 1953 through December 2009. "That’s 56 incredible years of Playboy - over 650 issues, more than 100,000 pages - all at your fingertips," reads the publisher’s promo copy.

Yes, there’s a "fingertips" joke in there somewhere. Feel free to share in the Comments section.

The Playboy drive comes with Bondi Digital Publishing’s magazine-browsing software, which is also used by magazine’s online archive of back issues.

The pocket-sized USB drive is compatible with both Mac and Windows PCs. Oh, yeah, it’s hot-swappable too.

Internet Explorer 6 Usage Plummets...Finally

Internet Explorer 6 was originally released in the summer of 2001. At the time, it was a significant step forward for Microsoft and helped to establish Internet Explorer as a dominant force in Web browsers. The

venerable browser has put up a good fight, but new usage statistics suggest it may finally be on its proverbial death bed.

Almost a decade and two major browser revisions after its launch, Internet Explorer 6 is almost universally criticized for its incompatibility with Web standards and its poor browser security. Despite the criticism, though, IE6 has refused to die. In fact, broken down by version, Internet Explorer 6 is still the number three browser, and has more market share than Internet Explorer 7.

Internet Explorer 9 in public beta and expected to be officially released sometime in the next year. Never mind any of the other improvements and features of these subsequent browsers, the security controls alone should be all the justification that organizations need to abandon IE6 and upgrade to IE8.

Apparently, all of the lobbying and anti-IE6 campaigns, combined with persistent prodding from Microsoft is finally paying off. Roger Capriotti, Director of Product Marketing for Internet Explorer, states in an Exploring IE blog post, "In the last six months, IE6 usage is now declining faster among enterprises than it is among worldwide consumers. We believe this reflects how organizations are recognizing the need to migrate to a modern browser."

Microsoft, with the help of Net Applications, has dug beneath the standard browser market share tracking to examine browser usage by organizations as opposed to individual consumers, and the results are encouraging. Small and medium businesses are leading the IE6 exodus, but overall only about 12 percent of browser usage in organizations - regardless of size - comes from IE6.

Many jump to the conclusion that Internet Explorer usage is directly linked with the market share of Microsoft Windows. The implication of that assumption being that IE6 is primarily still popular because Windows XP is still a dominant operating system. Capriotti explains, though, "While XP usage contributes to IE6 usage, the vast majority of commercial XP machines have already upgraded to IE7 or IE8. Less than 20 percent of web browsing on commercial XP machines comes from IE6."

One of the main reasons that organizations have been reluctant to upgrade from IE6 to IE8 is that they have nearly a decade of investment and development of custom business-critical applications that are designed to work with IE6. Migrating the browser requires also testing and updating those applications, which number in the thousands for some customers.

The reality of making the switch is not nearly as daunting as the apprehension would suggest, though. I spoke with Roger Capriotti and he told me that he hears regularly from customers that the process turned out to be much easier than had been anticipated, and that upgrading also provided an opportunity to inventory the apps that are out there and eliminate those that aren’t even used any more.

There are two ways for IT admins to approach the browser upgrade. One is to put it off and just migrate by attrition when moving from Windows XP to Windows 7. IE8 is the default browser in Windows 7 already, so no additional effort would be required. For organizations planning to switch to Windows 7 in the near future, this might be the way to go.

However, switching everything at once - which might also include a

hardware refresh - introduces a wide variety of variables simultaneously. If there are any issues with critical Web apps, troubleshooting will be more complicated. Organizations that are heavily invested in IE6 apps should consider upgrading the browser independently to focus specifically on the browser and minimize the number of moving parts involved.

=~=~=~=